

AMENDED IN ASSEMBLY JULY 2, 2015

AMENDED IN SENATE APRIL 22, 2015

SENATE BILL

No. 34

Introduced by Senator Hill
(Coauthor: Assembly Member Gatto)

December 1, 2014

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 34, as amended, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an "ALPR operator" as defined, including, among others, ~~ensuring that the information the~~

~~ALPR operator collects is protected with certain safeguards, and implementing and maintaining specified reasonable security procedures and practices to protect ALPR information and implementing a usage and privacy policy with respect to that information. information, as specified. The bill would impose similar requirements on an “ALPR end-user,” as defined.~~

The bill would require an ALPR operator that accesses or provides access to ALPR information to maintain a specified record of that access.

~~This bill would also require an “ALPR end-user,” as defined, to implement and maintain a specified usage and privacy policy.~~

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual who has been harmed by a violation of these provisions to bring a civil action in any court of competent jurisdiction against a person who knowingly caused ~~that violation. the harm.~~

The bill would require a public ~~agency~~ *agency, as defined*, that ~~considers implementing a program to gather information through the use of~~ *operates or intends to operate* an ALPR system to provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before ~~it implements implementing~~ the program. *The bill would also prohibit a public agency from selling, sharing, or transferring ALPR information, except to another public agency, as specified.*

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines “personal information” for these purposes to include an individual’s first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver’s license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information is not encrypted and is used in combination with an individual’s name, in the definition of “personal information” discussed above.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of California
7 whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person. The
9 disclosure shall be made in the most expedient time possible and
10 without unreasonable delay, consistent with the legitimate needs
11 of law enforcement, as provided in subdivision (c), or any measures
12 necessary to determine the scope of the breach and restore the
13 reasonable integrity of the data system.

14 (b) Any agency that maintains computerized data that includes
15 personal information that the agency does not own shall notify the
16 owner or licensee of the information of any breach of the security
17 of the data immediately following discovery, if the personal
18 information was, or is reasonably believed to have been, acquired
19 by an unauthorized person.

20 (c) The notification required by this section may be delayed if
21 a law enforcement agency determines that the notification will
22 impede a criminal investigation. The notification required by this
23 section shall be made after the law enforcement agency determines
24 that it will not compromise the investigation.

25 (d) Any agency that is required to issue a security breach
26 notification pursuant to this section shall meet all of the following
27 requirements:

28 (1) The security breach notification shall be written in plain
29 language.

30 (2) The security breach notification shall include, at a minimum,
31 the following information:

32 (A) The name and contact information of the reporting agency
33 subject to this section.

34 (B) A list of the types of personal information that were or are
35 reasonably believed to have been the subject of a breach.

1 (C) If the information is possible to determine at the time the
2 notice is provided, then any of the following: (i) the date of the
3 breach, (ii) the estimated date of the breach, or (iii) the date range
4 within which the breach occurred. The notification shall also
5 include the date of the notice.

6 (D) Whether the notification was delayed as a result of a law
7 enforcement investigation, if that information is possible to
8 determine at the time the notice is provided.

9 (E) A general description of the breach incident, if that
10 information is possible to determine at the time the notice is
11 provided.

12 (F) The toll-free telephone numbers and addresses of the major
13 credit reporting agencies, if the breach exposed a social security
14 number or a driver's license or California identification card
15 number.

16 (3) At the discretion of the agency, the security breach
17 notification may also include any of the following:

18 (A) Information about what the agency has done to protect
19 individuals whose information has been breached.

20 (B) Advice on steps that the person whose information has been
21 breached may take to protect himself or herself.

22 (4) In the case of a breach of the security of the system involving
23 personal information defined in paragraph (2) of subdivision (g)
24 for an online account, and no other personal information defined
25 in paragraph (1) of subdivision (g), the agency may comply with
26 this section by providing the security breach notification in
27 electronic or other form that directs the person whose personal
28 information has been breached to promptly change his or her
29 password and security question or answer, as applicable, or to take
30 other steps appropriate to protect the online account with the
31 agency and all other online accounts for which the person uses the
32 same user name or email address and password or security question
33 or answer.

34 (5) In the case of a breach of the security of the system involving
35 personal information defined in paragraph (2) of subdivision (g)
36 for login credentials of an email account furnished by the agency,
37 the agency shall not comply with this section by providing the
38 security breach notification to that email address, but may, instead,
39 comply with this section by providing notice by another method
40 described in subdivision (i) or by clear and conspicuous notice

1 delivered to the resident online when the resident is connected to
2 the online account from an Internet Protocol address or online
3 location from which the agency knows the resident customarily
4 accesses the account.

5 (e) Any agency that is required to issue a security breach
6 notification pursuant to this section to more than 500 California
7 residents as a result of a single breach of the security system shall
8 electronically submit a single sample copy of that security breach
9 notification, excluding any personally identifiable information, to
10 the Attorney General. A single sample copy of a security breach
11 notification shall not be deemed to be within subdivision (f) of
12 Section 6254 of the Government Code.

13 (f) For purposes of this section, “breach of the security of the
14 system” means unauthorized acquisition of computerized data that
15 compromises the security, confidentiality, or integrity of personal
16 information maintained by the agency. Good faith acquisition of
17 personal information by an employee or agent of the agency for
18 the purposes of the agency is not a breach of the security of the
19 system, provided that the personal information is not used or
20 subject to further unauthorized disclosure.

21 (g) For purposes of this section, “personal information” means
22 either of the following:

23 (1) An individual’s first name or first initial and last name in
24 combination with any one or more of the following data elements,
25 when either the name or the data elements are not encrypted:

26 (A) Social security number.

27 (B) Driver’s license number or California identification card
28 number.

29 (C) Account number, credit or debit card number, in
30 combination with any required security code, access code, or
31 password that would permit access to an individual’s financial
32 account.

33 (D) Medical information.

34 (E) Health insurance information.

35 (F) Information or data collected through the use or operation
36 of an automated license plate recognition system, as defined in
37 Section 1798.90.5.

38 (2) A user name or email address, in combination with a
39 password or security question and answer that would permit access
40 to an online account.

(h) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(i) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting of the notice on the agency’s Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section,

1 “agency” includes a local agency, as defined in subdivision (a) of
2 Section 6252 of the Government Code.

3 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

4 1798.82. (a) A person or business that conducts business in
5 California, and that owns or licenses computerized data that
6 includes personal information, shall disclose a breach of the
7 security of the system following discovery or notification of the
8 breach in the security of the data to a resident of California whose
9 unencrypted personal information was, or is reasonably believed
10 to have been, acquired by an unauthorized person. The disclosure
11 shall be made in the most expedient time possible and without
12 unreasonable delay, consistent with the legitimate needs of law
13 enforcement, as provided in subdivision (c), or any measures
14 necessary to determine the scope of the breach and restore the
15 reasonable integrity of the data system.

16 (b) A person or business that maintains computerized data that
17 includes personal information that the person or business does not
18 own shall notify the owner or licensee of the information of the
19 breach of the security of the data immediately following discovery,
20 if the personal information was, or is reasonably believed to have
21 been, acquired by an unauthorized person.

22 (c) The notification required by this section may be delayed if
23 a law enforcement agency determines that the notification will
24 impede a criminal investigation. The notification required by this
25 section shall be made promptly after the law enforcement agency
26 determines that it will not compromise the investigation.

27 (d) A person or business that is required to issue a security
28 breach notification pursuant to this section shall meet all of the
29 following requirements:

30 (1) The security breach notification shall be written in plain
31 language.

32 (2) The security breach notification shall include, at a minimum,
33 the following information:

34 (A) The name and contact information of the reporting person
35 or business subject to this section.

36 (B) A list of the types of personal information that were or are
37 reasonably believed to have been the subject of a breach.

38 (C) If the information is possible to determine at the time the
39 notice is provided, then any of the following: (i) the date of the
40 breach, (ii) the estimated date of the breach, or (iii) the date range

1 within which the breach occurred. The notification shall also
2 include the date of the notice.

3 (D) Whether notification was delayed as a result of a law
4 enforcement investigation, if that information is possible to
5 determine at the time the notice is provided.

6 (E) A general description of the breach incident, if that
7 information is possible to determine at the time the notice is
8 provided.

9 (F) The toll-free telephone numbers and addresses of the major
10 credit reporting agencies if the breach exposed a social security
11 number or a driver's license or California identification card
12 number.

13 (G) If the person or business providing the notification was the
14 source of the breach, an offer to provide appropriate identity theft
15 prevention and mitigation services, if any, shall be provided at no
16 cost to the affected person for not less than 12 months, along with
17 all information necessary to take advantage of the offer to any
18 person whose information was or may have been breached if the
19 breach exposed or may have exposed personal information defined
20 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

21 (3) At the discretion of the person or business, the security
22 breach notification may also include any of the following:

23 (A) Information about what the person or business has done to
24 protect individuals whose information has been breached.

25 (B) Advice on steps that the person whose information has been
26 breached may take to protect himself or herself.

27 (4) In the case of a breach of the security of the system involving
28 personal information defined in paragraph (2) of subdivision (h)
29 for an online account, and no other personal information defined
30 in paragraph (1) of subdivision (h), the person or business may
31 comply with this section by providing the security breach
32 notification in electronic or other form that directs the person whose
33 personal information has been breached promptly to change his
34 or her password and security question or answer, as applicable, or
35 to take other steps appropriate to protect the online account with
36 the person or business and all other online accounts for which the
37 person whose personal information has been breached uses the
38 same user name or email address and password or security question
39 or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, “personal information” means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject

1 persons to be notified exceeds 500,000, or the person or business
2 does not have sufficient contact information. Substitute notice
3 shall consist of all of the following:

4 (A) Email notice when the person or business has an email
5 address for the subject persons.

6 (B) Conspicuous posting of the notice on the Internet Web site
7 page of the person or business, if the person or business maintains
8 one.

9 (C) Notification to major statewide media.

10 (k) Notwithstanding subdivision (j), a person or business that
11 maintains its own notification procedures as part of an information
12 security policy for the treatment of personal information and is
13 otherwise consistent with the timing requirements of this part, shall
14 be deemed to be in compliance with the notification requirements
15 of this section if the person or business notifies subject persons in
16 accordance with its policies in the event of a breach of security of
17 the system.

18 SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5)
19 is added to Part 4 of Division 3 of the Civil Code, to read:

20
21 TITLE 1.81.23. COLLECTION OF LICENSE PLATE
22 INFORMATION
23

24 1798.90.5. The following definitions shall apply for purposes
25 of this title:

26 (a) “Automated license plate recognition end-user” or “ALPR
27 end-user” means a person that accesses or uses *an* ALPR
28 ~~information system~~, but does not include ~~a~~ *any of the following*:

29 (1) A transportation agency when subject to Section 31490 of
30 the Streets and Highways Code.

31 (2) *A person that is subject to Sections 6801 to 6809, inclusive,*
32 *of Title 15 of the United States Code and state or federal statutes*
33 *or regulations implementing those sections, if both of the following*
34 *apply:*

35 (A) *The person is subject to compliance oversight by a state or*
36 *federal regulatory agency with respect to those sections.*

37 (B) *The person has agreed to comply with and is subject to the*
38 *privacy policy of the ALPR operator providing the information.*

39 (3) *A person, other than a law enforcement agency, to whom*
40 *information may be disclosed as a permissible use pursuant to*

1 *Section 2721 of Title 18 of the United States Code, if the person*
2 *has agreed to comply with and is subject to the privacy policy of*
3 *the ALPR operator providing the information.*

4 (b) “Automated license plate recognition information,” or
5 “ALPR information” means information or data collected through
6 the use of an ALPR system.

7 (c) “Automated license plate recognition operator” or “ALPR
8 operator” means a person that operates an ALPR system, ~~or that~~
9 ~~stores or maintains ALPR information,~~ but does not include a
10 transportation agency when subject to Section 31490 of the Streets
11 and Highways Code.

12 (d) “Automated license plate recognition system” or “ALPR
13 system” means a ~~system~~ *searchable computerized database*
14 *resulting from the operation* of one or more mobile or fixed
15 cameras combined with computer algorithms to read and convert
16 images of registration plates and the characters they contain into
17 computer-readable data.

18 (e) “Person” ~~includes a law enforcement agency, government~~
19 ~~agency, private entity, or individual.~~ *means any natural person,*
20 *public agency, partnership, firm, association, corporation, limited*
21 *liability company, or other legal entity.*

22 (f) “Public agency” ~~means and includes every state agency and~~
23 ~~every local agency:~~ *the state, any city, county, or city and county,*
24 *or any agency or political subdivision of the state or a city, county,*
25 *or city and county, including, but not limited to, a law enforcement*
26 *agency.*

27 1798.90.51. An ALPR operator shall do all of the following:

28 (a) ~~(1) Ensure that ALPR information is protected with~~
29 ~~reasonable operational, administrative, technical, and physical~~
30 ~~safeguards to ensure its confidentiality and integrity.~~

31 ~~(2) Implement and maintain~~

32 (a) *Maintain* reasonable security procedures and ~~practices in~~
33 ~~order practices, including operational, administrative, technical,~~
34 ~~and physical safeguards,~~ to protect ALPR information from
35 unauthorized access, destruction, use, modification, or disclosure.

36 (b) (1) ~~Implement and maintain~~ a usage and privacy policy in
37 order to ensure that the collection, use, maintenance, sharing, and
38 dissemination of ALPR information is consistent with respect for
39 individuals’ privacy and civil liberties. The usage and privacy
40 policy shall be available *to the public* in writing, and, if the ALPR

1 operator has an Internet Web site, the usage and privacy policy
2 shall be posted conspicuously on that Internet Web site.

3 (2) The usage and privacy policy shall, at a minimum, include
4 all of the following:

5 (A) The authorized purposes for using *the ALPR-systems system*
6 and collecting ALPR information.

7 (B) A description of *the job title or other designation of* the
8 employees and independent contractors who are authorized to use
9 *or access the ALPR-systems, system, or to collect ALPR*
10 *information, and to access ALPR* information. The policy shall
11 identify the training requirements necessary for those authorized
12 employees and independent contractors.

13 (C) A description of how the ~~use of ALPR-systems system~~ will
14 be monitored to ensure *the security of the information and*
15 compliance with ~~all applicable privacy laws and a process for~~
16 ~~periodic system audits, including audits of the access log required~~
17 ~~by Section 1798.90.52: laws.~~

18 ~~(D) A description of reasonable measures that will be used to~~
19 ~~ensure the accuracy of ALPR information and a process to correct~~
20 ~~data errors.~~

21 ~~(E) A description of how the ALPR operator will comply with~~
22 ~~the security procedures and practices implemented and maintained~~
23 ~~pursuant to subdivision (a).~~

24 ~~(F) The length of time ALPR information will be stored or~~
25 ~~retained.~~

26 ~~(D) The purposes of, process for, and restrictions on, the sale,~~
27 ~~sharing, or transfer of ALPR information to other persons.~~

28 ~~(G)~~

29 ~~(E) The title of the official custodian, or owner, of the ALPR~~
30 ~~information and which employees and independent contractors~~
31 ~~have the responsibility and accountability for implementing~~
32 ~~subdivision (a) and this subdivision: system responsible for~~
33 ~~implementing this section.~~

34 ~~(H) The purpose of, and process for, sharing or disseminating~~
35 ~~ALPR information with other persons.~~

36 ~~(F) A description of the reasonable measures that will be used~~
37 ~~to ensure the accuracy of ALPR information and correct data~~
38 ~~errors.~~

1 (G) *The length of time ALPR information will be retained, and*
2 *the process the ALPR operator will utilize to determine if and when*
3 *to destroy retained ALPR information.*

4 1798.90.52. If an ALPR operator accesses or provides access
5 to ALPR information, the ALPR operator shall maintain a record
6 of that access. At a minimum, the record shall include all of the
7 following:

8 (a) The date and time the information is accessed.

9 (b) The license plate number or other data elements used to
10 query the ALPR ~~database or system.~~

11 (c) The ~~name~~ *username* of the person who accesses the
12 information, and, as applicable, the organization or entity with
13 whom the person is affiliated.

14 (d) The purpose for accessing the information.

15 1798.90.53. *An ALPR end-user shall do all of the following:*

16 (a) *Maintain reasonable security procedures and practices,*
17 *including operational, administrative, technical, and physical*
18 *safeguards, to protect ALPR information from unauthorized access,*
19 *destruction, use, modification, or disclosure.* ~~(a) An ALPR~~
20 ~~end-user shall implement and maintain~~

21 (b) (1) *Implement a usage and privacy policy in order to ensure*
22 *that the access, use, sharing, and dissemination of ALPR*
23 *information is consistent with respect for individuals' privacy and*
24 *civil liberties. The usage and privacy policy shall be available to*
25 *the public in writing, and, if the ALPR end-user has an Internet*
26 *Web site, the usage and privacy policy shall be posted*
27 *conspicuously on that Internet Web site.*

28 ~~(b)~~

29 (2) The usage and privacy policy shall, at a minimum, include
30 all of the following:

31 ~~(1)~~

32 (A) The authorized purposes for accessing and using ALPR
33 information.

34 ~~(2)~~

35 (B) A description of *the job title or other designation of* the
36 employees and independent contractors who are authorized to
37 access and use ALPR information. The policy shall identify the
38 training requirements necessary for those authorized employees
39 and independent contractors.

40 ~~(3)~~

1 (C) A description of how the ~~access and use of~~ ALPR
2 ~~information system~~ will be monitored to ensure *the security of the*
3 *information accessed or used*, and compliance with all applicable
4 privacy laws and a process for periodic system audits.

5 ~~(4) The length of time ALPR information will be retained by~~
6 ~~the ALPR end-user and the process the ALPR end-user will utilize~~
7 ~~to determine if and when to destroy the retained ALPR information.~~

8 (D) *The purposes of, process for, and restrictions on, the sale,*
9 *sharing, or transfer of ALPR information to other persons.*

10 ~~(5)~~

11 (E) *The title of the official custodian, or owner, of the ALPR*
12 ~~information. information responsible for implementing this section.~~

13 ~~(6) The purpose of, and process for, sharing or disseminating~~
14 ~~ALPR information with other persons.~~

15 ~~(7)~~

16 (F) A description of how the end-user will implement reasonable
17 security measures ~~to secure that will be used to ensure the accuracy~~
18 ~~of ALPR information from unauthorized access, destruction, use,~~
19 ~~modification, or disclosure. and correct data errors.~~

20 ~~(8) Which employees and independent contractors have the~~
21 ~~responsibility and accountability for implementing subdivision (a)~~
22 ~~and this subdivision.~~

23 (G) *The length of time ALPR information will be retained, and*
24 *the process the ALPR end-user will utilize to determine if and when*
25 *to destroy retained ALPR information.*

26 1798.90.54. (a) In addition to any other sanctions, penalties,
27 or remedies provided by law, an individual who has been harmed
28 by a violation of this ~~title~~ *title, including, but not limited to,*
29 *unauthorized access or use of ALPR information or a breach of*
30 *security of an ALPR system*, may bring a civil action in any court
31 of competent jurisdiction against a person who knowingly caused
32 ~~that violation. the harm.~~

33 (b) The court may award a combination of any one or more of
34 the following:

35 (1) Actual damages, but not less than liquidated damages in the
36 amount of two thousand five hundred dollars (\$2,500).

37 (2) Punitive damages upon proof of willful or reckless disregard
38 of the law.

39 (3) Reasonable attorney's fees and other litigation costs
40 reasonably incurred.

(4) Other preliminary and equitable relief as the court determines to be appropriate.

1798.90.55. Notwithstanding any other law or ~~regulation~~, a *regulation*:

(a) A public agency that ~~considers implementing a program to gather information through the use of~~ *operates or intends to operate* an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before it ~~implements~~ *implementing* the program.

(b) *A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. For purposes of this section, the provision of data hosting services shall not be considered the sale, sharing, or transferring of ALPR information.*

CORRECTIONS:

Text—Page 14.